Docket No. 245451US8/ims

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hideki KITAHAMA, et al. GAU:

SERIAL NO: 10/715,496 EXAMINER:

FILED: November 19, 2003

FOR: COMMUNICATION CONTROL APPARATUS, FIREWALL APPARATUS, AND DATA COMMUNICATION METHOD

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
JAPAN	2002-346271	November 28, 2002

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Joseph A. Scafetta Jr.

Bradley D. Lytle
Registration No. 40,073

Joseph A. Scafetta, Jr.
Registration No. 26, 803

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１１月２８日

出願番号
Application Number: 特願２００２－３４６２７１

[ST. 10/C]: [ＪＰ２００２－３４６２７１]

出願人
Applicant(s): 株式会社エヌ・ティ・ティ・ドコモ

２００３年１１月１９日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０９５７１６

【書類名】　特許願
【整理番号】　14-0428
【提出日】　平成14年11月28日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 13/00
【発明者】
　【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
　【氏名】　北濱　秀基
【発明者】
　【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
　【氏名】　石田　創
【特許出願人】
　【識別番号】　392026693
　【氏名又は名称】　株式会社エヌ・ティ・ティ・ドコモ
【代理人】
　【識別番号】　100088155
　【弁理士】
　【氏名又は名称】　長谷川　芳樹
【選任した代理人】
　【識別番号】　100092657
　【弁理士】
　【氏名又は名称】　寺崎　史朗
【選任した代理人】
　【識別番号】　100114270
　【弁理士】
　【氏名又は名称】　黒川　朋也

【選任した代理人】

【識別番号】　100108213

【弁理士】

【氏名又は名称】　阿部　豊隆

【選任した代理人】

【識別番号】　100113549

【弁理士】

【氏名又は名称】　鈴木　守

【手数料の表示】

【予納台帳番号】　014708

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　通信制御装置、ファイアウォール装置、通信制御システム、及び、データ通信方法

【特許請求の範囲】

【請求項１】

移動機を接続可能な複数のファイアウォール装置とデータの送受信を行う通信制御装置において、

前記移動機に適したファイアウォール設定情報を、当該移動機の識別情報と対応付けて格納する格納手段と、

前記移動機の接続先のファイアウォール装置を検知する検知手段と、

前記移動機の接続先のファイアウォール装置を検知したことに伴い、前記移動機の識別情報に対応するファイアウォール設定情報を、前記ファイアウォール装置宛に送信する送信手段と

を備えることを特徴とする通信制御装置。

【請求項２】

請求項１に記載の通信制御装置と複数の移動機との間におけるデータ送受信を中継するファイアウォール装置において、

前記ファイアウォール設定情報に含まれるフィルタリング条件を各移動機の識別情報と対応付けて保持する保持手段と、

前記通信制御装置から送信されるパケットの宛先である移動機を識別する識別手段と、

前記識別手段により識別された移動機に対応するフィルタリング条件に従って、前記パケットの通過許否を判定する判定手段と

を備えることを特徴とするファイアウォール装置。

【請求項３】

請求項１に記載の通信制御装置と、請求項２に記載のファイアウォール装置とを備え、

前記移動機は、受信するパケットを、前記ファイアウォール装置を経由して受信することを特徴とする通信制御システム。

【請求項４】

移動機に適したファイアウォール設定情報を、当該移動機の識別情報と対応付けて格納する格納手段を備える通信制御装置が、前記移動機を接続可能な複数のファイアウォール装置とデータの送受信を行うデータ通信方法において、

前記通信制御装置の検知手段が、前記移動機の接続先のファイアウォール装置を検知する検知ステップと、

前記通信制御装置の送信手段が、前記移動機の接続先のファイアウォール装置を検知したことに伴い、前記移動機の識別情報に対応するファイアウォール設定情報を、前記ファイアウォール装置宛に送信する送信ステップと

を含むことを特徴とするデータ通信方法。

【請求項５】

ファイアウォール装置が、請求項１に記載の通信制御装置と複数の移動機との間におけるデータ送受信を中継するデータ通信方法において、

前記ファイアウォール装置の保持手段が、前記ファイアウォール設定情報に含まれるフィルタリング条件を各移動機の識別情報と対応付けて保持する保持ステップと、

前記ファイアウォール装置の識別手段が、前記通信制御装置から送信されるパケットの宛先である移動機を識別する識別ステップと、

前記ファイアウォール装置の判定手段が、前記識別ステップにて識別された移動機に対応するフィルタリング条件に従って、前記パケットの通過許否を判定する判定ステップと

を含むことを特徴とするデータ通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信制御装置、ファイアウォール装置、通信制御システム、及び、データ通信方法に関する。

【０００２】

【従来の技術】

従来、携帯電話などの移動機が、その移動に関わらず同一のＩＰ（Internet Protocol）アドレスを使用する技術であるモバイルＩＰｖ６がＩＥＴＦ（Internet Engineering Task Force）において検討されている。モバイルＩＰｖ６は、移動機としてのモバイルＩＰ端末とホームエージェントとにより実現される。宛先アドレスがモバイルＩＰ端末の恒久的なＩＰアドレス（ホームアドレス）であるパケットは、通常のＩＰの手順で転送された後、ホームエージェントのあるリンクに到達する。これにより、ホームエージェントは、ホームアドレス宛のパケットを受信する。

【０００３】

モバイルＩＰ端末は、移動すると、移動先のノードで、既存のステートレスアドレス自動生成技術（ＲＦＣ２４６２）やステートフルアドレス自動生成技術（ＤＨＣＰ：Dynamic Host Configuration Protocol）を使用して、一時的なＩＰアドレスである気付アドレスを取得する。モバイルＩＰ端末は、この気付アドレスをホームエージェントに登録する。

【０００４】

モバイルＩＰ端末が他の端末と通信を行う方法には、双方向トンネルモードと経路最適化モードとの２つの方法がある。双方向トンネルモードでは、モバイルＩＰ端末とホームエージェントとの間にトンネルが生成される。トンネルとは、ＲＦＣ２４７３に開示されている様に、元のＩＰパケットを別のＩＰパケットに包含して送信することにより、元のＩＰパケットの送信元ＩＰアドレスや宛先ＩＰアドレスとは無関係に、任意の経路でパケットを運ぶ技術である。

【０００５】

モバイルＩＰ端末から他の端末に向けてＩＰパケットを送信する場合には、このＩＰパケットは、トンネルを経由して、まずホームエージェント宛に送信される。ホームエージェントは、ＩＰパケットをトンネルから出した後、通常のＩＰの手順により他の端末宛に送出する。これにより、ＩＰパケットは、他の端末に到達する。反対に、他の端末からモバイルＩＰ端末に向けてＩＰパケットを送信する場合には、ＩＰパケットは、通常のＩＰの手順によりホームエージェントに到達する。その後、ホームエージェントは、このＩＰパケットをトンネルに入れ

て、モバイルＩＰ端末宛に送出する。

【０００６】

これに対して、経路最適化モードでは、モバイルＩＰ端末は、ＩＰパケットの送信に先立って、他の端末にＩＰアドレスを通知する。ＩＰパケットが双方向トンネルモードにより他の端末からモバイルＩＰ端末宛に送信された場合、モバイルＩＰ端末は、経路最適化モードにモード変更するために、自端末の気付アドレスを上記他の端末宛に送信する。

【０００７】

経路最適化モードにおいて、モバイルＩＰ端末から他の端末に向けてＩＰパケットを送信する場合には、このＩＰパケットは、モバイルＩＰ端末から他の端末宛に直接（トンネルを経由せずに）送信される。このとき、ＩＰパケットの送信元アドレスには気付アドレスが設定されており、ＩＰパケット内のホームアドレスオプションにはホームアドレスが設定されている。

【０００８】

一方、他の端末からモバイルＩＰ端末に向けてＩＰパケットを送信する場合には、ＩＰパケットにルーチングヘッダが付され、ＩＰパケットは、他の端末からモバイルＩＰ端末に直接に（トンネルを経由せずに）送信される。なお、ルーチングヘッダは、ＲＦＣ２４６０により規定されており、任意の中継点を経由してパケットを送信するための情報である。ＩＰパケットの第１の宛先（中継点）としては気付アドレスが設定され、第２の宛先としてはホームアドレスが設定される。

【０００９】

また、ＬＡＮ等の内部ネットワークでは、インターネット等の外部ネットワークからの不正アクセスを検出及び遮断するために、所定のフィルタリング条件に従って、各ネットワークの境界に到達したデータの通過許否を判定するファイアウォールを設置する。ファイアウォールは、多くの場合ソフトウェアの形で提供され、ルータやプロキシサーバ等に組み込まれて使用されるが、高い性能が要求されるため、専用のハードウェアが用いられる場合もある（例えば、特許文献１参照。）。

【００１０】

【特許文献１】

特開平１０－７０５７６

【００１１】

【発明が解決しようとする課題】

ファイアウォールは、高価で高度な設定技術が必要なため専門家以外による運用が困難である上に、以下の理由などから、主に企業内ＬＡＮを守るために使用されていた。すなわち、ダイヤルアップ接続を行う端末や携帯電話などの移動機は、外部ネットワークに接続する場所が状況や用途に応じて異なるので、ファイアウォールの適切かつ固定的な設置場所の特定が困難である。また、ダイヤルアップ接続を行う端末は、割り当てられるＩＰアドレスが接続時毎に異なるので、接続時毎にフィルタリングの条件を変更する必要があり実用的ではない。更に、ダイヤルアップ接続は、接続時間が短いため、その間にインターネットから攻撃される可能性は低く、端末をファイアウォールで守らなくてもトラブルに合うことは殆どなかった。

【００１２】

更に、近年では、個人ユーザが使用する端末が常時接続により外部ネットワークと接続する形態が増加しており、この様な端末に関しても、ファイアウォールを使用する必要性が高まってきた。ところが、かかる端末としての、携帯電話やノートパソコン等の携帯型通信端末（以下、「移動機」と記す。）は、接続先のノードが高頻度かつ高速に変化することが想定されるため、設置位置が不変的なファイアウォールを使用できない。

【００１３】

そこで、本発明の課題は、移動機に対するファイアウォール機能の適用を可能とすることである。

【００１４】

【課題を解決するための手段】

上記課題を解決するために、本発明に係る通信制御装置は、移動機を接続可能な複数のファイアウォール装置とデータの送受信を行う通信制御装置において、

前記移動機に適したファイアウォール設定情報を、当該移動機の識別情報と対応付けて格納する格納手段と、前記移動機の接続先のファイアウォール装置を検知する検知手段と、前記移動機の接続先のファイアウォール装置を検知したことに伴い、前記移動機の識別情報に対応するファイアウォール設定情報を前記ファイアウォール装置宛に送信する送信手段とを備える。

【００１５】

本発明に係るデータ通信方法は、移動機に適したファイアウォール設定情報を、当該移動機の識別情報と対応付けて格納する格納手段を備える通信制御装置が、前記移動機を接続可能な複数のファイアウォール装置とデータの送受信を行うデータ通信方法において、前記通信制御装置の検知手段が、前記移動機の接続先のファイアウォール装置を検知する検知ステップと、前記通信制御装置の送信手段が、前記移動機の接続先のファイアウォール装置を検知したことに伴い、前記移動機の識別情報に対応するファイアウォール設定情報を前記ファイアウォール装置宛に送信する送信ステップとを含む。

【００１６】

これらの発明によれば、移動機の接続先のファイアウォール装置が検知されたことに伴い、前記移動機の識別情報に対応するファイアウォール設定情報が、前記移動機の新規接続先のファイアウォール装置宛に送信される。これにより、移動機に適したファイアウォール設定情報は、移動機の接続先のファイアウォール装置に送信され設定される。

【００１７】

したがって、移動機がファイアウォール装置に初期接続した場合にはもとより、移動機が移動により接続先のファイアウォール装置を変更した場合にも、ファイアウォール設定情報は、接続先変更後のファイアウォール装置に送信され設定される。つまり、ファイアウォール設定情報は、移動機の移動に追従する。ファイアウォール設定情報には、上記移動機宛のパケットのフィルタリング条件が含まれているので、ファイアウォール装置に到達した上記パケットに関しては、かかるフィルタリング条件に従って通過の許否（転送又は破棄）が判定される。その結果、移動機に対しても、適切なファイアウォール機能の適用が可能となる。

【００１８】

本発明に係るファイアウォール装置は、上述した通信制御装置と複数の移動機との間におけるデータ送受信を中継するファイアウォール装置において、前記ファイアウォール設定情報に含まれるフィルタリング条件を各移動機の識別情報と対応付けて保持する保持手段と、前記通信制御装置から送信されるパケットの宛先である移動機を識別する識別手段と、前記識別手段により識別された移動機に対応するフィルタリング条件に従って、前記パケットの通過許否を判定する判定手段とを備える。

【００１９】

本発明に係るデータ通信方法は、ファイアウォール装置が、上述した通信制御装置と複数の移動機との間におけるデータ送受信を中継するデータ通信方法において、前記ファイアウォール装置の保持手段が、前記ファイアウォール設定情報に含まれるフィルタリング条件を各移動機の識別情報と対応付けて保持する保持ステップと、前記ファイアウォール装置の識別手段が、前記通信制御装置から送信されるパケットの宛先である移動機を識別する識別ステップと、前記ファイアウォール装置の判定手段が、前記識別ステップにて識別された移動機に対応するフィルタリング条件に従って、前記パケットの通過許否を判定する判定ステップとを含む。

【００２０】

これらの発明によれば、ファイアウォール設定情報に含まれるフィルタリング条件が各移動機の識別情報と対応付けて保持された後、通信制御装置からファイアウォール装置に送信されたパケットの宛先である移動機が識別され、該移動機に対応するフィルタリング条件に従って、前記パケットの通過許否が判定される。これにより、ファイアウォール装置に到達したパケットの通過許否の判定に際して使用されるフィルタリング条件が移動機毎に適宜変更される。したがって、当該パケットが宛先となる可能性のない移動機に関してまで、通過許否判定処理が不要に行われることが防止される。その結果、ファイアウォール装置を使用する移動機が増加しても、各移動機宛のパケットの伝送遅延時間の増大を抑制することが可能となる。

【００２１】

本発明に係る通信制御システムは、上述した通信制御装置と上述したファイアウォール装置とを備え、前記移動機は、受信するパケットを前記ファイアウォール装置を経由して受信する。

【００２２】

【発明の実施の形態】

（第１の実施形態）

以下、本発明の第１の実施形態について、図面を参照して詳細に説明する。

図１は、本発明に係る通信制御システム１の全体構成を示す図である。図１に示す様に、通信制御システム１は、ホームエージェント装置１０（通信制御装置に対応）と三台のファイアウォール装置２０，３０，４０（複数のファイアウォール装置に対応）と移動機５０とを備えて構成される。

【００２３】

ホームエージェント装置１０と移動機５０とは、三台のファイアウォール装置２０～４０の内の任意の１台を少なくとも経由して、相互に各種データの送受信が可能な様に接続されている。インターネット等の外部ネットワークから送信されたＩＰパケットは、ホームエージェント装置１０により一旦受信された後、移動機５０の現在位置の最も近傍に位置するファイアウォール装置２０により中継され、当該ＩＰパケットの宛先である移動機５０に到達可能である。

【００２４】

図２は、本発明に係るホームエージェント装置１０の機能的構成を示す図である。図２に示す様に、ホームエージェント装置１０は、設定ファイル元データ格納部１１（格納手段に対応）と、ＢＵ受信部１２（検知手段に対応）と、設定ファイル送信部１３（送信手段に対応）とを備える。各部はバスを介して、各部の機能に応じた信号の入出力が可能な様に接続されている。

【００２５】

以下、ホームエージェント装置１０の各構成要素について詳細に説明する。

設定ファイル元データ格納部１１には、後述の設定ファイル元データ（ファイアウォール設定情報に対応）が、移動機識別情報と対応付けて格納されている。

移動機識別情報は、例えば、移動機のホームアドレスやＭＡＣアドレスである。

【００２６】

設定ファイル元データには、例えば以下に示す情報が記述されている。

①．ファイアウォール名

②．「外部ネットワークから来るＩＰパケットの振分け基準」の生成に必要な情報

③．「移動機から送信されるＩＰパケットの振分け基準」の生成に必要な情報

④．「アクセス制御リスト」の生成に必要な情報

【００２７】

すなわち、①の情報は、ファイアウォールの設定内容を一意に特定可能な情報であり、既に送信済の又は作成時から所定時間経過した設定ファイル元データをホームエージェント装置１０が削除する際に使用される。

②の情報は、外部ネットワークからホームエージェント装置１０を経由して送信されるＩＰパケットの宛先となる移動機をファイアウォール装置が識別するための情報である。②の情報は、必要に応じて記述される。かかる情報は、例えば、移動機５０のＩＰアドレスであるが、必ずしも１つのＩＰアドレスに限らず、複数の宛先ＩＰアドレスが範囲指定されたものであってもよい。

【００２８】

③の情報は、移動機から送信されるＩＰパケットの送信元をファイアウォール装置が識別するための情報である。かかる情報は、例えば、送信元ＭＡＣアドレスを振分け基準にするか送信元ＩＰアドレスを振分け基準にするかを指定するための情報や、ＭＡＣアドレスを振分け基準にする場合のＭＡＣアドレスである。

【００２９】

④の情報は、ファイアウォール装置がＩＰパケットの通過許否を判定する際に使用されるフィルタリング条件が記載された周知慣用のアクセス制御リストの生成に必要な情報である。例えば、アクセス制御リストの元になるリストと、該リスト上のどの部分を気付アドレスに書き換えるかを指定するための情報である。但し、アクセス制御リストには、②及び③の情報に基づいて識別される移動機宛のＩＰパケットの通過許否判定に使用されるフィルタリング条件が記載されてお

り、その他の移動機に関するフィルタリング条件は記載されていない。これにより、通過許否判定に伴う検索データ量を減らし、パケットフィルタリング処理の高速化を図る。アクセス制御リストは、最上行からの順次検索が可能な様に行単位で記載されており、各行の先頭項目から順に、ＩＰパケットの通過の可否を示す“ｄｅｎｙ”又は“ｐｅｒｍｉｔ”、ＩＰパケットの上位層プロトコル、ＩＰパケットの送信元アドレス及び送信元ポート番号、ＩＰパケットの宛先アドレス及び宛先ポート番号などが記載されている。

【００３０】

ＢＵ受信部１２は、移動機５０が移動した旨を通知するためのパケットであるバインディングアップデート（ＢＵ：Binding Update）を、移動先のファイアウォール装置２０から受信する。ＢＵ受信部１２は、このバインディングアップデートの受信により、移動機５０がファイアウォール装置と接続したこと（接続先の変更を含む）を検知し、その旨を設定ファイル送信部１３に通知する。

【００３１】

設定ファイル送信部１３は、移動機５０の接続がＢＵ受信部１２から通知されると、上記バインディングアップデートを参照して、ファイアウォール装置と接続した移動機を特定する。設定ファイル送信部１３は、特定された移動機の識別情報及び対応する設定ファイル元データを設定ファイル元データ格納部１１から取得し、設定ファイル元データを元に設定ファイルを生成する。設定ファイル送信部１３は、上記移動機識別情報及び設定ファイルをバインディングアック（ＢＡ：Binding Acknowledgement）と共に、移動機５０の新規接続先であるファイアウォール装置宛に送信する。バインディングアックとは、バインディングアップデートに対する確認応答信号である。

【００３２】

図３は、本発明に係るファイアウォール装置２０の機能的構成を示す図である。ファイアウォール装置２０は、アクセスルータを始めとするルータ自体であってもよいし、ルータとは別体に構成されたファイアウォール専用の端末であってもよい。図３に示す様に、ファイアウォール装置２０は、パケット振分け部２１，２４（識別手段に対応）と、ファイアウォールプロセス２２１，２２２，２２

３（保持手段及び判定手段に対応）と、出力バッファ２３，２５とを備える。各部はバスを介して、各部の機能に応じた信号の入出力が可能な様に接続されている。

【００３３】

パケット振分け部２１は、ホームエージェント装置１０から送信された移動機識別情報及び設定ファイルを受信すると、該移動機識別情報に基づいて設定ファイルの設定先となるファイアウォールプロセスを特定する。該当するファイアウォールプロセスがない場合には、ファイアウォールプロセスを生成する。特定又は生成されたファイアウォールプロセスには、上記移動機識別情報及び設定ファイルが保持される。また、パケット振分け部２１には、設定ファイル内のファイアウォール名、及び外部ネットワークから来るＩＰパケットの振分け基準が設定される。パケット振分け部２４には、設定ファイル内のファイアウォール名、及び移動機から送信されるＩＰパケットの振分け基準が設定される。

【００３４】

その後、パケット振分け部２１は、外部ネットワークから送信されたＩＰパケットを受信すると、設定された振分け基準に従って、当該ＩＰパケットを、その宛先移動機に対応するファイアウォールに出力する。同様に、パケット振分け部２４は、移動機から送信されたＩＰパケットを受信すると、設定された振分け基準に従って、当該ＩＰパケットを、その送信元移動機に対応するファイアウォールプロセスに出力する。

【００３５】

また、外部ネットワークから移動機５０に向かう方向（下り方向）にＩＰパケットが送信される場合には、ファイアウォールプロセス２２１は、通過許否の判定に先立って、パケット振分け部２１から取得されたＩＰパケットから、以下の１～３に示す手順で、フィルタリング用の宛先ＩＰアドレス及び送信元ＩＰアドレスを取得する。

【００３６】

１．ＩＰパケットが双方向トンネルモードにより送信されている場合、すなわち、外側のＩＰパケットの送信元アドレスがホームエージェントアドレスであり

、宛先アドレスが気付アドレスであり、ＩＰパケットがＩＰパケットを内包する場合には、ファイアウォールプロセス２２１は、内部のＩＰパケットを取得し、該ＩＰパケットに対して、下記の２及び３に示す手順を適用する。一方、ＩＰパケットが双方向トンネルモードにより送信されていない場合には、ファイアウォールプロセス２２１は、パケット振分け部２１から取得されたＩＰパケットに対して、そのまま下記の２及び３に示す手順を適用する。

【００３７】

２．ＩＰパケットが経路最適化モードにより移動機５０宛に送信されている場合、すなわち、ＩＰパケットの宛先アドレスが気付アドレスであり、ルーチングヘッダが存在し、該ルーチングヘッダに設定されている第２の宛先がホームアドレスである場合には、ファイアウォールプロセス２２１は、フィルタリング用の宛先ＩＰアドレスとしてホームアドレスを使用する。一方、ＩＰパケットが経路最適化モードにより移動機５０宛に送信されていない場合には、ファイアウォールプロセス２２１は、ＩＰパケットの宛先アドレスをフィルタリング用の宛先ＩＰアドレスとしてそのまま使用する。

【００３８】

３．ＩＰパケットが経路最適化モードによりモバイルＩＰ端末から送信されている場合、すなわち、ＩＰパケットの送信元アドレスが気付アドレスであり、ホームアドレスオプションが設定されている場合には、ファイアウォールプロセス２２１は、該ホームアドレスオプションに設定されているアドレスを、フィルタリング用の送信元ＩＰアドレスとして使用する。一方、ＩＰパケットが経路最適化モードによりモバイルＩＰ端末から送信されていない場合には、ファイアウォールプロセス２２１は、ＩＰパケットの送信元アドレスをフィルタリング用の送信元ＩＰアドレスとしてそのまま使用する。

【００３９】

移動機５０から外部ネットワークに向かう方向（上り方向）にＩＰパケットが送信される場合には、ファイアウォールプロセス２２１は、通過許否の判定に先立って、パケット振分け部２４から取得されたＩＰパケットから、以下の１～３に示す手順で、フィルタリング用の宛先ＩＰアドレス及び送信元ＩＰアドレスを

取得する。

【００４０】

１．ＩＰパケットが双方向トンネルモードにより送信されている場合、すなわち、外側のＩＰパケットの送信元アドレスが気付アドレスであり、宛先アドレスがホームエージェントアドレスであり、ＩＰパケットがＩＰパケットを内包する場合には、ファイアウォールプロセス２２１は、内部のＩＰパケットを取得し、該ＩＰパケットに対して、下記の２及び３に示す手順を適用する。一方、ＩＰパケットが双方向トンネルモードにより送信されていない場合には、ファイアウォールプロセス２２１は、パケット振分け部２４から取得されたＩＰパケットに対して、そのまま下記の２及び３に示す手順を適用する。

【００４１】

２．ＩＰパケットが経路最適化モードによりモバイルＩＰ端末宛に送信されている場合、すなわち、ＩＰパケット内にルーチングヘッダが存在する場合には、ファイアウォールプロセス２２１は、該ルーチングヘッダに設定されている第２の宛先をフィルタリング用の宛先ＩＰアドレスとして使用する。一方、ＩＰパケットが経路最適化モードによりモバイルＩＰ端末宛に送信されていない場合には、ファイアウォールプロセス２２１は、ＩＰパケットの宛先アドレスをフィルタリング用の宛先ＩＰアドレスとしてそのまま使用する。

【００４２】

３．ＩＰパケットが経路最適化モードにより移動機５０から送信されている場合、すなわち、ＩＰパケットの送信元アドレスが気付アドレスであり、ホームアドレスオプションが設定されている場合には、ファイアウォールプロセス２２１は、該ホームアドレスオプションに設定されているアドレスを、フィルタリング用の送信元ＩＰアドレスとして使用する。一方、ＩＰパケットが経路最適化モードにより移動機５０から送信されていない場合には、ファイアウォールプロセス２２１は、ＩＰパケットの送信元アドレスをフィルタリング用の送信元ＩＰアドレスとしてそのまま使用する。

【００４３】

更に、ファイアウォールプロセス２２１は、上記の手順で取得されたフィルタ

リング用の宛先ＩＰアドレス及び送信元ＩＰアドレスを使用して、設定ファイル内のアクセス制御リストに記載されているフィルタリング条件に従って、パケット振分け部２１により振り分けられたＩＰパケットの通過許否を判定する。通過が許可されたＩＰパケットは出力バッファ２３に出力され、通過が拒否されたＩＰパケットは破棄される。これにより、ファイアウォールプロセス２２１は、宛先又は送信元が移動機５０であるＩＰパケットのフィルタリングを実現する。

【００４４】

ファイアウォールプロセス２２２は、上述したファイアウォールプロセス２２１と同一の機能的構成を有する。すなわち、ファイアウォールプロセス２２２は、移動機５０とは別の移動機である移動機６０（図示せず）の識別情報及び設定ファイルを保持し、宛先又は送信元アドレスが移動機６０であるＩＰパケットのフィルタリングを実現する。ファイアウォールプロセス２２３に関しても同様に、更に別の移動機である移動機７０（図示せず）の識別情報及び設定ファイルを保持し、宛先又は送信元が移動機７０であるＩＰパケットのフィルタリングを実現する。

【００４５】

出力バッファ２３は、ファイアウォールプロセス２２１～２２３の何れかから入力されたＩＰパケットを、当該ＩＰパケットの宛先である移動機宛に無線チャネルを介して送信（転送）する。

【００４６】

パケット振分け部２４は、上述したパケット振分け部２１と機能的構成を同一とするが、パケット振分け部２１とはＩＰパケットの送信方向が異なる。すなわち、パケット振分け部２１が、ホームエージェント装置１０側に形成されたインターネット等の外部ネットワークからＩＰパケットを受信するのに対して、パケット振分け部２４は、移動機５０側から送信されたＩＰパケットを受信する。

【００４７】

出力バッファ２５は、ファイアウォールプロセス２２１～２２３の何れかから入力されたＩＰパケットを、当該ＩＰパケットの宛先のノードに送信（転送）する。

ファイアウォール装置３０，４０は、ファイアウォール装置２０と設置位置が異なるものの、構成に関しては、上述したファイアウォール装置２０と同様であるので、その説明は省略する。

【００４８】

移動機５０は、Mobile IPv6に準拠した移動ノードである。移動機５０は、電源投入や長期断線後の再接続に伴い、ファイアウォール装置２０～４０の内、最も受信レベルの高いファイアウォール装置と無線接続する。本実施の形態では特に、通信制御システム１内のファイアウォール装置２０に移動機５０が新規に接続（初期接続）する場合を想定するが、移動に伴って、接続先のファイアウォール装置を変更（ハンドオーバ）することも勿論可能である。

【００４９】

移動機５０は、ファイアウォール装置と接続すると、当該ファイアウォール装置を経由してホームエージェント装置１０宛に上記バインディングアップデートを送信する。また、移動機５０は、ホームエージェント装置１０から送信される上記バインディングアックを受信する。

【００５０】

次に、図４及び図５を参照して、通信制御システム１の動作を説明する。併せて、本発明に係るデータ通信方法を構成する各ステップについて説明する。

図４は、通信制御システム１により実行制御されるファイアウォール構築処理を説明するためのフローチャートである。

【００５１】

まず、Ｓ１では、移動機５０は、電源が投入されたり、長期断線後に再接続されたことを契機として、ファイアウォール装置２０～４０の内、最も受信レベルの高い（通常は最も近傍に位置する）ファイアウォール装置２０と無線接続する。

【００５２】

Ｓ２では、移動機５０は、周知慣用のMobile IPv6の接続手順に従って、ファイアウォール装置２０との無線接続が完了した旨を通知すべく、バインディングアップデートをホームエージェント装置１０宛に送信する。このバインディング

アップデートには、送信元である移動機５０の識別情報が少なくとも含まれている。

【００５３】

Ｓ３では、ホームエージェント装置１０は、ＢＵ受信部１２により、移動機５０から送信されたバインディングアップデートを受信する。

Ｓ４では、ホームエージェント装置１０は、設定ファイル送信部１３により、上記バインディングアップデートに含まれる送信元移動機の識別情報を基に、移動機５０の識別情報及びこれに対応する設定ファイル元データを設定ファイル元データ格納部１１から取得する。

【００５４】

Ｓ５では、ホームエージェント装置１０は、設定ファイル送信部１３により、Ｓ４で取得された設定ファイル元データを元に、以下のＩ～Ｖに示す手順で設定ファイルを生成する。

【００５５】

Ｉ．ファイアウォール名を設定ファイル元データからコピーする。

ＩＩ．「外部ネットワークから来るＩＰパケットの振分け基準」として、気付アドレスを設定する。

ＩＩＩ．送信元ＩＰアドレスを振分け基準にする様に指定されている場合には、「移動機から送信されるＩＰパケットの振分け基準」として、ホームアドレスと気付アドレスとを設定する。送信元ＭＡＣアドレスを振分け基準にする様に指定されている場合には、「移動機から送信されるＩＰパケットの振分け基準」として、設定ファイル元データのＭＡＣアドレスをコピーする。

ＩＶ．アクセス制御リストの元になるリスト上において書き換えが指定されている部分を気付アドレスに置換し、「アクセス制御リスト」として設定する。

Ｖ．「ホームエージェントアドレス」として、ホームエージェントのＩＰアドレスを設定する。

【００５６】

Ｓ６では、ホームエージェント装置１０は、設定ファイル送信部１３により、Ｓ４で取得された移動機５０の識別情報及びＳ５で生成された設定ファイルをバ

インディングアックに添付して、移動機５０宛に送信する。

【００５７】

なお、本実施の形態では、設定ファイルは、ホームエージェント装置１０側で生成及び送信されるものとして説明した。しかし、ホームエージェント装置１０がファイアウォール装置宛に設定ファイル元データを送信し、ファイアウォール装置が、この設定ファイル元データを元に設定ファイルを生成するものとしてもよい。

【００５８】

移動機５０は、ファイアウォール装置２０と接続されているので、移動機５０宛のバインディングアックは、ファイアウォール装置２０を必然的に経由する。Ｓ７では、ファイアウォール装置２０は、送信途中のバインディングアックに添付されている、移動機５０の識別情報及び設定ファイルを取得する。

Ｓ８では、移動機５０がバインディングアックを受信し、これを以って、移動機５０のホームエージェント装置１０に対する位置登録が完了する。このとき、移動機５０は、バインディングアックと共に上記設定ファイルを受信してもよい。

【００５９】

なお、移動機識別情報及び設定ファイルは、バインディングアックに乗せて送信されるものとしたが、バインディングアックとは別に送信されるものとしてもよい。すなわち、ホームエージェント装置１０が、バインディングアップデートの気付アドレスを基に、移動機５０が接続しているファイアウォール装置２０のプレフィクスを割り出し、該プレフィクスの示すネットワーク上の全てのファイアウォール装置に対して設定ファイルをマルチキャストする。その後、ホームエージェント装置１０は、移動機５０宛にバインディングアックを送信する。

【００６０】

Ｓ９においては、ファイアウォール装置２０は、Ｓ７で取得された移動機５０の識別情報及び設定ファイルを使用して、移動機５０用のファイアウォールプロセス２２１を生成する。Ｓ９におけるファイアウォールの生成とは、設定ファイル内のアクセス制御リストを実行するプロセスを特定の移動機用にカスタマイズ

することである。ファイアウォールの生成に際して、上記プロセスの初期化（内部変数の設定）が必要であればこれを実行し、移動前の動作状態が設定ファイル内に存在すれば、これを上記プロセスの内部変数に設定する。

【００６１】

Ｓ１０では、ファイアウォール装置２０は、Ｓ７で取得された設定ファイルからファイアウォール名及び振分け基準を取得し、パケット振分け部２１及び２４に設定する。

以上、移動機５０に適用されるファイアウォールを構築する過程について説明したが、移動機６０，７０に適用されるファイアウォールに関しても同様のステップを経て構築される。

【００６２】

続いて、図５を参照して、ファイアウォール構築後のファイアウォール装置２０により実行制御されるＩＰパケットフィルタリング処理について説明する。

以下、ホームエージェント１０から移動機５０に向かう方向（下り方向）にＩＰパケットが送信される場合を想定して説明するが、これとは反対方向（上り方向）にＩＰパケットが送信される場合に関しても同様の処理を実行可能である。

【００６３】

Ｔ１では、パケット振分け部２１により、ＩＰパケットの受信の有無が監視される。

Ｔ２では、パケット振分け部２１により、ＩＰパケットのヘッダ情報から宛先ＩＰアドレスが特定されると共に、該アドレスを有する移動機に対応するファイアウォールを振分け先として上記ＩＰパケットが出力される。例えば、受信されたＩＰパケットの宛先ＩＰアドレスが移動機５０のＩＰアドレスである場合には、ＩＰパケットはファイアウォールプロセス２２１に振り分けられる。

【００６４】

このとき、受信されたＩＰパケットの振分け先となるファイアウォールが未生成の状況が懸念されるが、かかる場合には、事前に設定された処理（以下、「デフォルト処理」と記す。）が実行される。デフォルト処理としては、例えば、ファイアウォール装置２０がＩＰパケットの記述内容を検査し、記述内容がホーム

エージェント装置１０へのバインディングアップデートであれば、当該パケットをホームエージェント装置１０に送信する。バインディングアップデートでない場合にはその時点でＩＰパケットを破棄する。

【００６５】

Ｔ３では、ファイアウォールプロセス２２１により、図４のＳ９で生成された上記プロセスに基づいて、ＩＰパケットの通過許否が判定される。なお、ファイアウォールプロセス２２１は、ＩＰパケットの通過許否判定処理に限らず、通過優先順位の設定、認証情報の検査、記述内容の変更などの処理を実行するものとしてもよい。

【００６６】

Ｔ３における判定の結果、通過が許可されると（Ｔ４；Ｙｅｓ）、ファイアウォールプロセス２２１により、ＩＰパケットが出力バッファ２３に出力及び保持される（Ｔ５）。そして、Ｔ６では、出力バッファ２３に保持されているＩＰパケットは、ファイアウォール装置２０と移動機５０とを接続する無線チャネルを介して、移動機５０宛に送信される。

【００６７】

一方、Ｔ３における判定の結果、通過が拒否されると（Ｔ４；Ｎｏ）、ファイアウォールプロセス２２１により、ＩＰパケットは削除される（Ｔ７）。このとき、ＩＰパケットが削除された旨が、その送信元であるホームエージェント装置１０に通知されるものとしてもよい。

【００６８】

Ｔ６又はＴ７の処理終了後、ファイアウォール装置２０は、更なるＩＰパケットの受信を待機すべく、Ｔ１に戻り、Ｔ１以降の処理を再び実行する。

以上、通信制御システム１が移動機５０宛のＩＰパケットに対してフィルタリングを行う過程について説明したが、移動機６０，７０宛のＩＰパケットに対するフィルタリング処理に関しても同様のステップを経ることにより実行可能である。これにより、専用のファイアウォールが生成された全ての移動機宛のＩＰパケットに関して、高速かつ適確な通過許否判定が可能となる。

【００６９】

上述した様に、本発明に係る通信制御システム１によれば、移動機が直接的に接続する可能性のある端末の位置にファイアウォールを配備する。ホームエージェント装置１０が、任意の移動機から送信されたバインディングアップデートを受信すると、当該移動機に適したファイアウォールの設定ファイルを上記ファイアウォール装置宛に送信する。ファイアウォール装置は、この設定ファイルを使用して、上記移動機に適したファイアウォールを生成する。これにより、移動機が接続した任意のファイアウォール装置に、当該移動機用のファイアウォールが構築されることになり、移動する端末へのファイアウォール機能の適用が可能となる。

【００７０】

ここで、移動機に対してファイアウォール機能を適用した場合、移動機を利用するユーザの増加に伴って、フィルタリング条件が指定されたアクセス制御リストの記載量が膨大になることが予測される。一方で、ファイアウォール装置は、パケットの通過許否判定に際して、アクセス制御リストの最上行から順番にヘッダ情報と条件との照合を行う。このため、上記記載量の増加に伴って通過許否判定の処理時間が長くなり、パケットの伝送遅延時間が増大することが懸念される。

【００７１】

かかる懸念を解消するためには、ファイアウォール装置が、移動機毎に異なるフィルタリング条件を使用することが有効である。フィルタリング条件を移動機毎に変更する手法としては、物理的なインタフェースを移動機毎に変えることも考えられる。しかしながら、この手法では、無線ＬＡＮに代表されるレイヤ２での接続の様に、同一の物理インタフェースを多数の移動機で共有する場合への適用が極めて困難である。

【００７２】

そこで、フィルタリング条件を移動機毎に変更するために、ファイアウォール装置は、パケットを受信すると、当該パケットの宛先となる移動機を識別し、該識別結果に応じて、パケットに適用するファイアウォールを適宜変更する。これにより、パケットが送信される可能性のない移動機に関して、不必要な通過許否

判定が行われることが未然に防止される。したがって、移動機の増加に伴うパケットの伝送遅延時間の増大が抑制される。その結果、転送処理速度を低下させることなく、移動機に対してファイアウォール機能を適用することが可能となる。

【００７３】

（第２の実施形態）

以下、本発明の第２の実施形態について、図面を参照して詳細に説明する。

第１の実施形態では、移動機５０が通信制御システム１内のファイアウォール装置に初期接続した場合を想定した。このため、ファイアウォール装置は、ホームエージェント装置が生成した設定ファイルを受信して使用するものとした。これに対して、本実施の形態では、移動機５０が移動により接続先のファイアウォール装置を変更（ハンドオーバ）した場合を想定し、移動元のファイアウォール装置に保持されている設定ファイルを移動先のファイアウォール装置が受信して使用する。

【００７４】

以下、本実施の形態における通信制御システムについて詳細に説明する。

本実施形態における通信制御システムの構成は、第１の実施形態において詳述した通信制御システムの構成と同様である。したがって、各構成要素には同一の符合を付すと共にその説明は省略する。本実施の形態では、移動機５０が、ファイアウォール装置２０からファイアウォール装置３０へ接続先を変更した場合を想定する。

【００７５】

次に、図６を参照して、通信制御システム１により実行されるファイアウォール構築処理について説明する。

移動機５０が接続先のファイアウォール装置を変更すると（Ｓ１１）、ホームエージェント装置１０宛にバインディングアップデートを送信する（Ｓ１２）。

ホームエージェント装置１０は、バインディングアップデートを移動機５０から受信すると（Ｓ１３）、移動元のファイアウォール装置２０のＩＰアドレスを移動先のファイアウォール装置３０へ送信する（Ｓ１４）。このＩＰアドレスは、移動機５０がファイアウォール装置２０に接続した際、つまり移動前に、バイ

ンディングアップデートと共に通知される。

【００７６】

ファイアウォール装置３０は、ファイアウォール装置２０のＩＰアドレスを受信したことを契機として（Ｓ１５）、当該アドレス宛に、移動機５０用の設定ファイルの転送要求を送信する（Ｓ１６）。

ファイアウォール装置２０は、上記転送要求をファイアウォール装置３０から受信すると（Ｓ１７）、ファイアウォールプロセス２２１に保持していた移動機５０の識別情報及び設定ファイルをファイアウォール装置３０に向けて送信する（Ｓ１８）。

【００７７】

ファイアウォール装置３０は、移動機５０の識別情報及び設定ファイルをファイアウォール装置２０から受信すると（Ｓ１９）、当該設定ファイルを使用して、移動機５０用のファイアウォールを生成する（Ｓ２０）。

以下、図４に示したＳ１０と同様の処理が実行される。すなわち、パケット振分け部２１に、ファイアウォール名及び振分け基準が設定される。

【００７８】

上述した様に、移動機５０は、ハンドオーバに伴ってホームエージェント装置１０宛にバインディングアップデートを送信する。したがって、移動機５０が接続先のファイアウォール装置を変更する度、つまり移動機５０が移動する度に、当該移動機に適したフィルタリング条件を有するファイアウォールの位置が可変的に制御される。結果として、ファイアウォールが移動機５０の変位に追随することになり、移動する端末へのファイアウォール機能の適用が可能となる。

【００７９】

移動機５０の移動先にファイアウォールを構築する手法としては様々な態様が考えられるが、通信負荷を極力抑制して効率的なファイアウォール構築を行う観点から、移動前のファイアウォール装置に既存の設定ファイルを移動後のファイアウォール装置に転用することが好適である。すなわち、移動先のファイアウォール装置３０が、移動機５０の設定ファイルを既に保持するファイアウォール装置のＩＰアドレスをホームエージェント装置１０から取得すると共に、当該ファ

イアウォール装置から上記設定ファイルを取得する。これにより、ホームエージェント装置１０とファイアウォール装置３０との間で設定ファイルの送受信を行うことなく、移動後の移動機５０に対してファイアウォール機能を適用することができる。ＩＰアドレスは、設定ファイルと比較してデータ容量が小さいので、通信制御システム１における通信負荷を低減することが可能となる。

【００８０】

（第３の実施形態）

以下、移動機５０が、移動により接続先のファイアウォール装置を変更した場合における更に別の態様としての第３の実施形態について、図面を参照して詳細に説明する。ここで、本実施形態における通信制御システムの構成は、第１の実施形態において詳述した通信制御システムの構成と同様であるので、各構成要素には同一の符合を付すと共にその説明は省略する。また、本実施の形態では、第２の実施形態と同様に、移動機５０が、ファイアウォール装置２０からファイアウォール装置３０にハンドオーバした場合を想定する。

【００８１】

図７を参照して、通信制御システム１により実行されるファイアウォール構築処理について説明する。

本実施の形態において通信制御システム１により実行されるファイアウォール構築処理は、第２の実施形態において詳述したファイアウォール構築処理（図６参照）と共通するステップを複数含む。具体的には、図７のＳ２１～Ｓ２３，Ｓ２９，及びＳ３０以降の各ステップは、図６に示したＳ１１～Ｓ１３，Ｓ１９，及びＳ２０以降の各ステップにそれぞれ相当する。

【００８２】

以下、本実施の形態に特有のステップであるＳ２４～Ｓ２８（図７中太線で示す処理）について説明する。すなわち、ホームエージェント装置１０は、バインディングアップデートを移動機５０から受信したことを契機として、移動元のファイアウォール装置２０宛に、移動機５０用の設定ファイルの転送要求を送信する（Ｓ２４）。

ファイアウォール装置２０は、上記転送要求をホームエージェント装置１０か

ら受信すると（Ｓ２５）、ファイアウォールプロセス２２１に保持していた移動機５０の識別情報及び設定ファイルを一旦ホームエージェント装置１０へ送信する（Ｓ２６）。

【００８３】

ホームエージェント装置１０は、移動機５０の識別情報及び設定ファイルをファイアウォール装置２０から受信すると（Ｓ２７）、これらの情報を、移動先のファイアウォール装置３０宛に送信（転送）する（Ｓ２８）。以下、図６に示したＳ１９と同様の処理が実行される。すなわち、パケット振分け部２１及び２４に、ファイアウォール名及び振分け基準が設定される。

かかる態様を採ることによっても、通信制御システム１は、ファイアウォールの位置を可変的に制御することができ、移動機５０の移動元から移動先にファイアウォールを追随させることが可能となる。

【００８４】

（第４の実施形態）

以下、移動機５０が、移動により接続先のファイアウォール装置を変更した場合における更に別の態様としての第４の実施形態について、図面を参照して詳細に説明する。ここで、本実施形態における通信制御システムの構成は、第１の実施形態において詳述した通信制御システムの構成と同様であるので、各構成要素には同一の符合を付すと共にその説明は省略する。また、本実施の形態では、第２及び第３の実施形態と同様に、移動機５０が、ファイアウォール装置２０からファイアウォール装置３０にハンドオーバした場合を想定する。

【００８５】

図８を参照して、通信制御システム１により実行されるファイアウォール構築処理について説明する。

本実施の形態において通信制御システム１により実行されるファイアウォール構築処理は、第３の実施形態において詳述したファイアウォール構築処理（図７参照）と共通するステップを複数含む。具体的には、図８のＳ３１～Ｓ３５，Ｓ３７，及びＳ３８以降の各ステップは、図７に示したＳ２１～Ｓ２５，Ｓ２９，及びＳ３０以降の各ステップにそれぞれ相当する。

【００８６】

以下、本実施の形態に特有のステップであるＳ３６（図８中太線で示す処理）について説明する。すなわち、Ｓ３６においては、移動元のファイアウォール装置２０は、ホームエージェント装置１０から設定ファイルの転送要求を受信したことを契機として、ファイアウォールプロセス２２１に保持していた移動機５０の識別情報及び設定ファイルをマルチキャストする。

【００８７】

ここで、マルチキャスト先のアドレスとしては、ホームエージェント装置１０から通知されたＩＰアドレスが使用される。すなわち、ホームエージェント装置１０は、Ｓ３３で受信されたバインディングアップデートの気付アドレスに基づいて、移動機５０が接続していたファイアウォール装置２０のプレフィクスを割り出し、当該プレフィクスの示すネットワーク上の全てのファイアウォール装置をマルチキャスト先として選択する。その後、ホームエージェント装置１０は、選択されたマルチキャスト先のＩＰアドレスを転送要求と共に、ファイアウォール装置２０に通知する。これにより、ファイアウォール装置２０は、システム内における他のファイアウォール装置３０，４０に対するマルチキャストを実行可能となる。

【００８８】

ファイアウォール装置２０からマルチキャストされた、移動機５０の識別情報及び設定ファイルは、上記ネットワーク上のファイアウォール装置３０により受信され、ファイアウォールの生成に使用される。ファイアウォール装置４０宛にマルチキャストされた、移動機５０の識別情報及び設定ファイルは、移動機５０がファイアウォール装置４０に接続先を変更した場合におけるファイアウォールの生成に使用することができる。

かかる態様を採ることによっても、通信制御システム１は、ファイアウォールの位置を可変的に制御することができ、移動機５０の移動元から移動先にファイアウォールを追随させることが可能となる。

【００８９】

（第５の実施形態）

以下、移動機５０が、移動により接続先のファイアウォール装置を変更した場合における更に別の態様としての第５の実施形態について、図面を参照して詳細に説明する。ここで、本実施形態における通信制御システムの構成は、第１の実施形態において詳述した通信制御システムの構成と同様であるので、各構成要素には同一の符合を付すと共にその説明は省略する。また、本実施の形態では、第２～第４の実施形態と同様に、移動機５０が、ファイアウォール装置２０からファイアウォール装置３０にハンドオーバした場合を想定する。

【００９０】

図９を参照して、通信制御システム１により実行されるファイアウォール構築処理について説明する。

本実施の形態において通信制御システム１により実行されるファイアウォール構築処理は、第２の実施形態において詳述したファイアウォール構築処理（図６参照）と共通するステップを複数含む。具体的には、図９のＳ４１，Ｓ４４，Ｓ４５～Ｓ４９以降の各ステップは、図６に示したＳ１１，Ｓ１３，Ｓ１６～Ｓ２０以降の各ステップにそれぞれ相当する。

【００９１】

以下、本実施の形態に特有のステップであるＳ４２，Ｓ４３（図９中太線で示す処理）について説明する。すなわち、Ｓ４２においては、移動機５０は、バインディングアップデート、及び移動前にホームエージェント装置１０から送信された設定ファイル（以下、「旧設定ファイル」と記す。）をホームエージェント装置１０宛に送信する。

【００９２】

Ｓ４３では、移動先のファイアウォール装置３０は、上記旧設定ファイルを参照して、移動元のファイアウォール装置２０のＩＰアドレスを認識する。これにより、ファイアウォール装置３０は、移動機５０の識別情報及び設定ファイルの転送要求先を特定することができる。続いて、ファイアウォール装置３０は、転送要求先であるファイアウォール装置２０から、上記識別情報及び設定ファイルを受信して、移動機５０用のファイアウォールを生成する。したがって、ファイアウォールの位置を可変的に制御することができ、移動機５０の移動にファイア

ウォールを追随させることが可能となる。

【００９３】

上述した様に、第２～第５の実施形態では、移動元のファイアウォール装置から移動先のファイアウォール装置に、設定ファイル等の情報の転送を行っているが、この目的は以下に示す通りである。

【００９４】

第一の目的は、ファイアウォール装置が内部状態又はグローバル変数をもっている場合に、この状態を引き継ぐことである。例えば、移動機は、ＴＣＰ（Transmission Control Protocol）の接続信号を受信すると、ＴＣＰに関するデータを記憶し、ＴＣＰの切断信号を受信するとデータを消去し、通信中でないのにデータを受信すると破棄する、といった動作をする。かかる動作を移動機に適用する場合、移動機に記憶されたデータを移動先に引き継ぐ必要がある。

【００９５】

第二の目的は、情報の転送の最小化を図ることである。すなわち、アクセス制御リストに関しては、移動機１台分の情報といえども、データ容量が大きくなることがあり得る。また、ホームエージェント装置は、移動機（又はファイアウォール装置）から遠い位置に存在することが多いが、ハンドオーバ時における移動元のファイアウォール装置と移動先のファイアウォール装置とは極めて近い位置に存在する可能性が高い。このため、第２、第４、及び第５の実施形態に示した様に、移動元のファイアウォール装置から移動先のファイアウォール装置に情報を送信すると、ネットワーク負荷が低減される可能性がある。

【００９６】

なお、本発明は、上述した実施の形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲において、適宜変形態様を採ることも可能である。例えば、本実施の形態では、ファイアウォールの設定ファイルを生成及び送信する主体は、ホームエージェント装置としたが、ホームエージェント機能を有する装置とは別体に構成されたサーバ装置であってもよい。

【００９７】

特に、移動機に対してＲＡＤＩＵＳ（Remote Authentication Dial-In User S

ervice）認証を行う場合には、認証時に移動機の移動が検知できるので、ＲＡＤＩＵＳサーバが設定ファイルを生成及び送信してもよい。

【００９８】

以下、ホームエージェント装置の代わりにＲＡＤＩＵＳサーバを使用した態様について説明する。まず、ＲＡＤＩＵＳは、ＲＦＣ２８６５により標準化されている技術であるので、詳細な説明は省略し基本的な手順について簡単に説明する。ユーザ端末からリモートアクセス装置に対して、電話による遠隔接続の要求があると、リモートアクセス装置は、ＲＡＤＩＵＳサーバにアクセス要求メッセージを送信する。通常、このアクセス要求メッセージには、ユーザ端末にて入力されたユーザＩＤやパスワードが含まれている。ＲＡＤＩＵＳサーバは、ユーザＩＤやパスワードに基づいてユーザの検証を行い、検証結果に応じたメッセージ（アクセス許可メッセージ又はアクセス許否メッセージ）を返信する。リモートアクセス装置は、このメッセージに従って、遠隔接続の実行又は電話の切断を行う。

【００９９】

また、上記手順が規定されたプロトコルは、以下の様に拡張された。一つの拡張は、アクセス許可メッセージとしてのパケットに様々なデータを乗せることである。様々なデータとは、例えば、ユーザ端末が遠隔接続可能な最大時間、使用されるＩＰアドレス、フィルタリングＩＤ等である。他の拡張は、ＲＡＤＩＵＳをリモートアクセス以外に使用することである。例えば、リモートアクセス装置の代わりに無線ＬＡＮ基地局を使用すれば、無線ＬＡＮの利用者認証にＲＡＤＩＵＳを使用することができる。

【０１００】

以下、上記拡張技術を勘案して、ＲＡＤＩＵＳが適用された通信制御システムの構成及び動作を説明する。通信制御システムは、移動機と、無線基地局を兼ねるファイアウォール装置（基地局兼ファイアウォール）と、ＲＡＤＩＵＳサーバとを少なくとも備えて構成される。移動機は、報知情報を受信すると、その送信元である基地局兼ファイアウォールに対して、基地局への接続要求を送信する。基地局兼ファイアウォールは、当該接続要求の受信に伴い、ＲＡＤＩＵＳサーバ

にアクセス要求を送信する。

【０１０１】

アクセス要求を受けたＲＡＤＩＵＳサーバは、上記移動機に関してユーザ検証を行い、検証の結果アクセス許可が得られると、当該移動機用のファイアウォールの設定ファイルを生成する。そして、アクセス許可メッセージ（パケット）に上記設定ファイルを乗せて、基地局兼ファイアウォール宛に送信する。基地局兼ファイアウォールは、設定ファイルを参照してファイアウォールプロセスを初期化した後、移動機による基地局への接続を許可する。

【０１０２】

すなわち、移動機は、移動する度に、新たな通信エリアの無線基地局との通信許可をとり、通信許可が得られた場合には、この無線基地局にファイアウォールが設定される。なお、ファイアウォールの設定に関するＲＡＤＩＵＳサーバの動作は、上記各実施形態にて詳述したホームエージェント装置の動作と同様であるので、その説明は省略する。

【０１０３】

更に、本実施の形態では、移動機は、単体の装置であるものとして説明したが、複数の装置が回線により接続された移動式ネットワークであってもよい。この場合、複数の装置は同時かつ同様に移動することになり、インターネット等の外部ネットワークからは１つの端末として認識される。移動式ネットワークと外部ネットワークとを接続する装置は例えばルータである。

【０１０４】

【発明の効果】

本発明によれば、移動機に対するファイアウォール機能の適用が可能となる。

【図面の簡単な説明】

【図１】

通信制御システムの全体構成を示す図である。

【図２】

ホームエージェント装置の機能的構成を示すブロック図である。

【図３】

ファイアウォール装置の機能的構成を示すブロック図である。

【図４】

第１の実施形態におけるファイアウォール構築処理を説明するためのフローチャートである。

【図５】

ＩＰパケットフィルタリング処理を説明するためのフローチャートである。

【図６】

第２の実施形態におけるファイアウォール構築処理を説明するためのフローチャートである。

【図７】

第３の実施形態におけるファイアウォール構築処理を説明するためのフローチャートである。

【図８】

第４の実施形態におけるファイアウォール構築処理を説明するためのフローチャートである。

【図９】

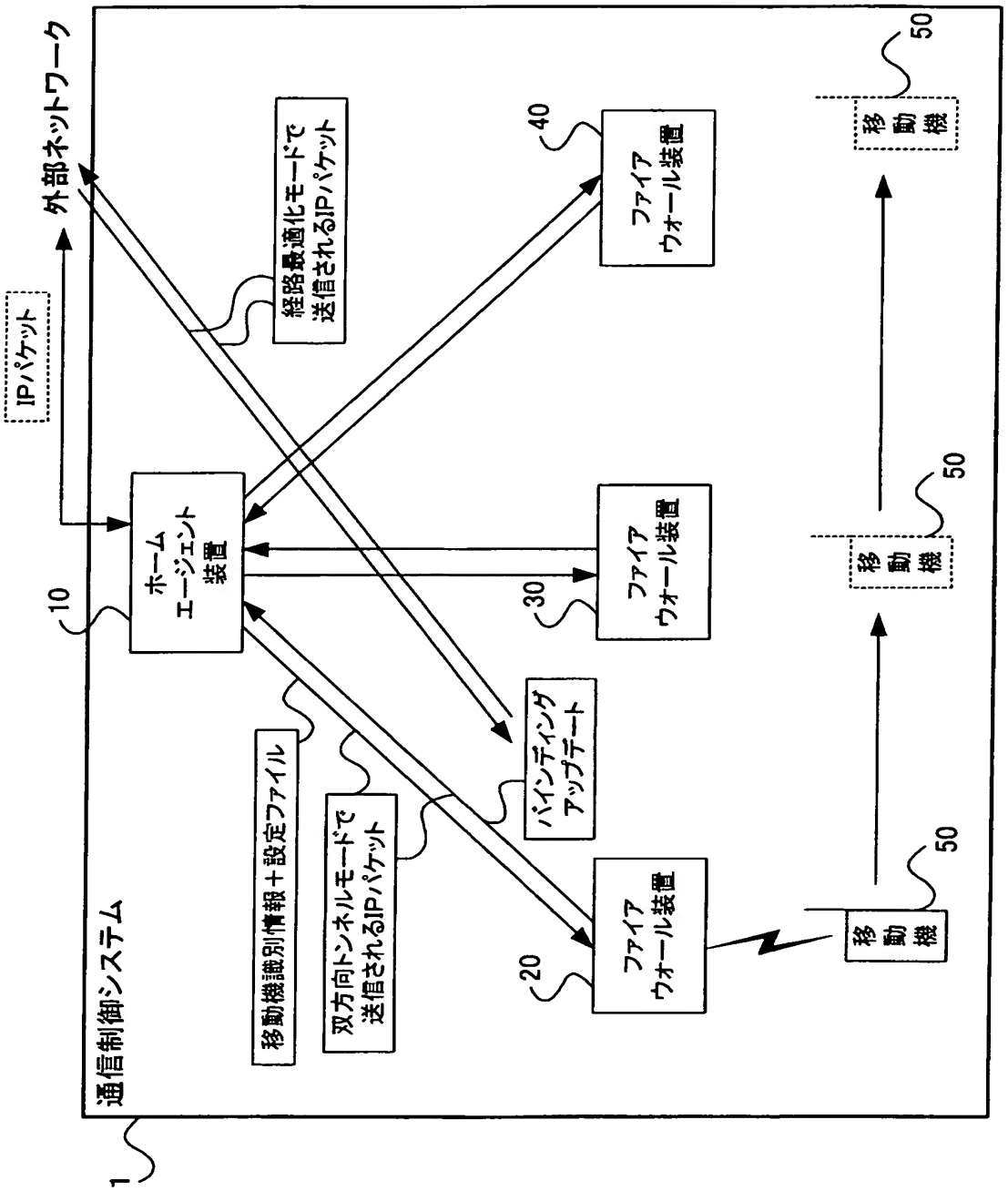
第５の実施形態におけるファイアウォール構築処理を説明するためのフローチャートである。

【符号の説明】

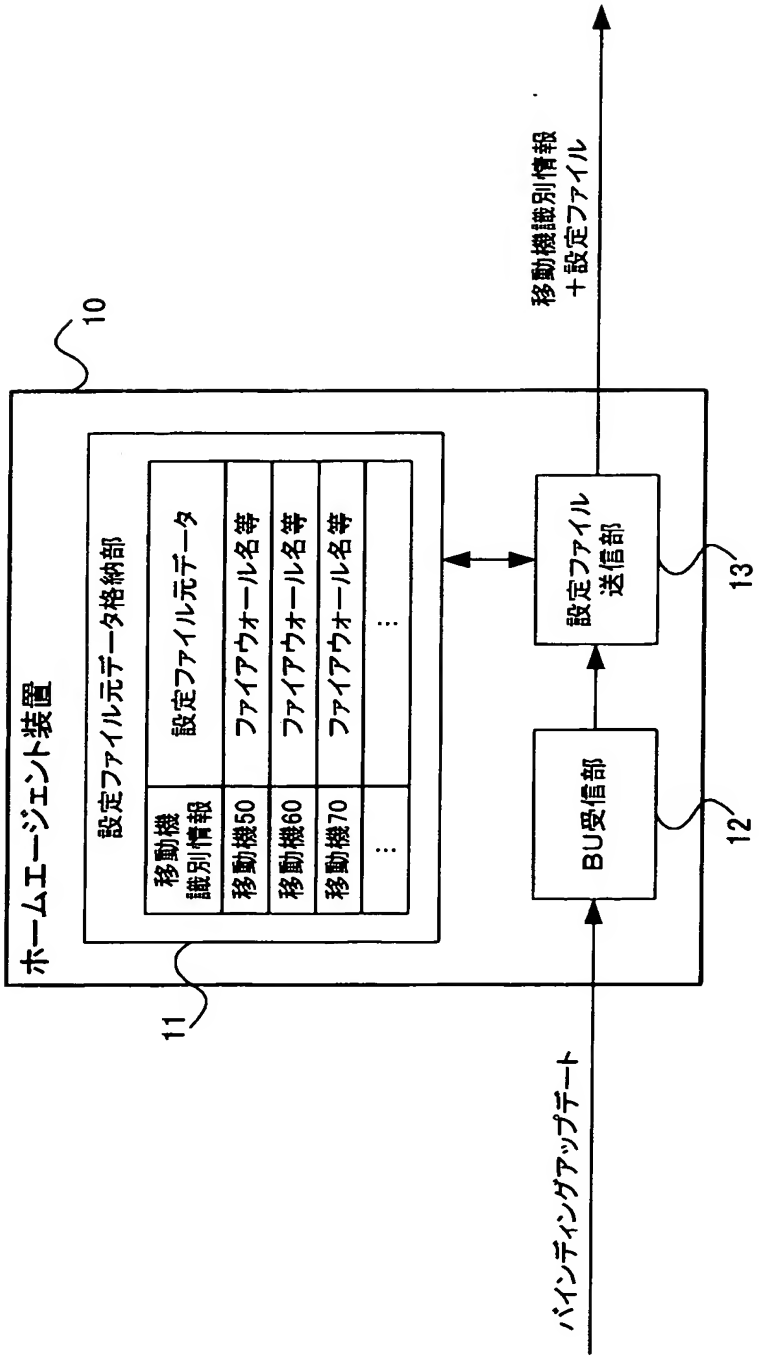
１…通信制御システム、１０…ホームエージェント装置、１１…設定ファイル元データ格納部、１２…ＢＵ受信部、１３…設定ファイル送信部、２０，３０，４０…ファイアウォール装置、２１，２４…パケット振分け部、２２１，２２２，２２３…ファイアウォールプロセス、２３，２５…出力バッファ、５０…移動機

【書類名】　図面

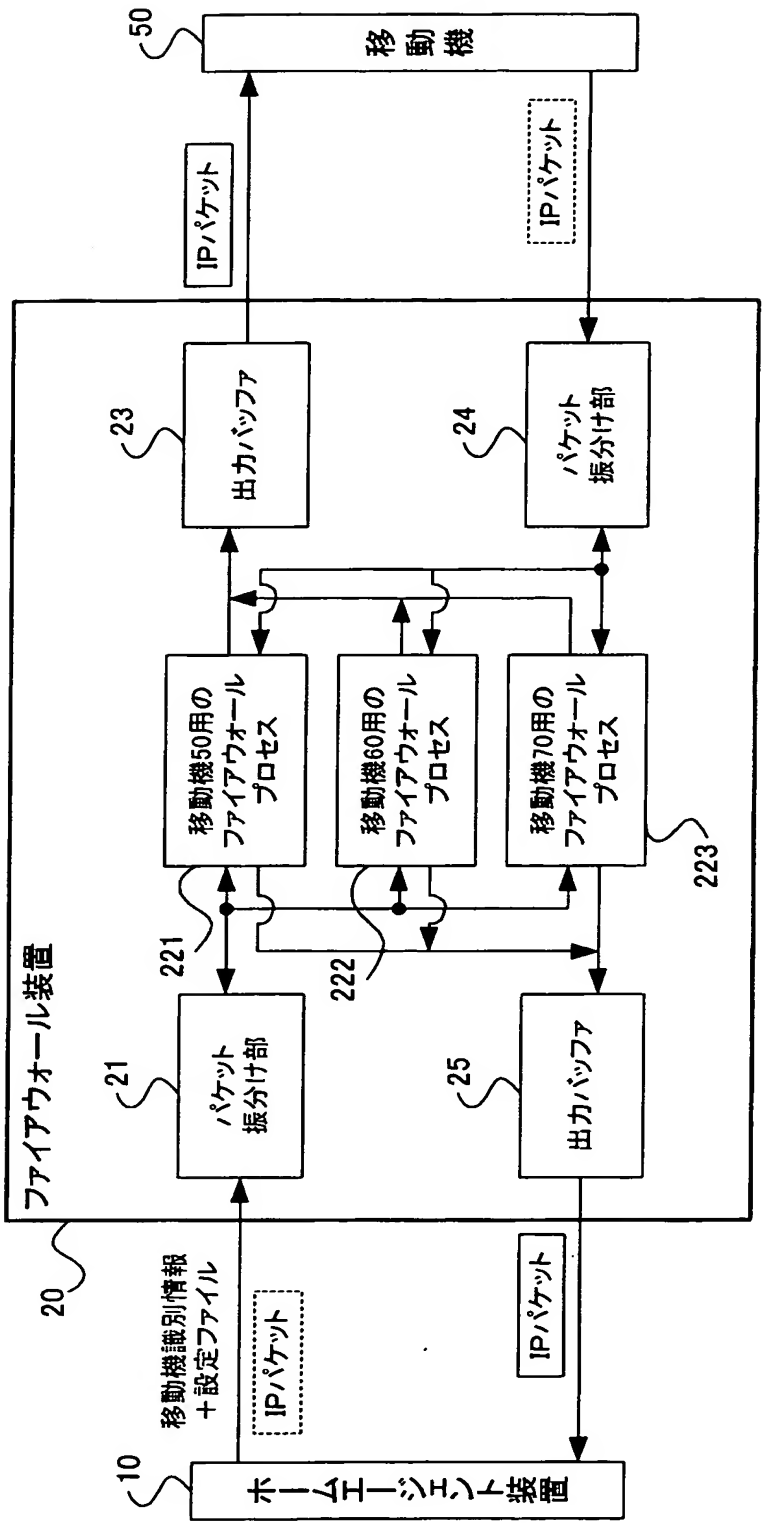
【図１】


外部ネットワーク
IPパケット
通信制御システム
1
ホーム
エージェント
装置
10
ファイア
ウォール装置
20
ファイア
ウォール装置
30
ファイア
ウォール装置
40
経路最適化モードで
送信されるIPパケット
移動機識別情報＋設定ファイル
双方向トンネルモードで
送信されるIPパケット
バインディング
アップデート
移動
機
50
移動
機
50
移動
機
50

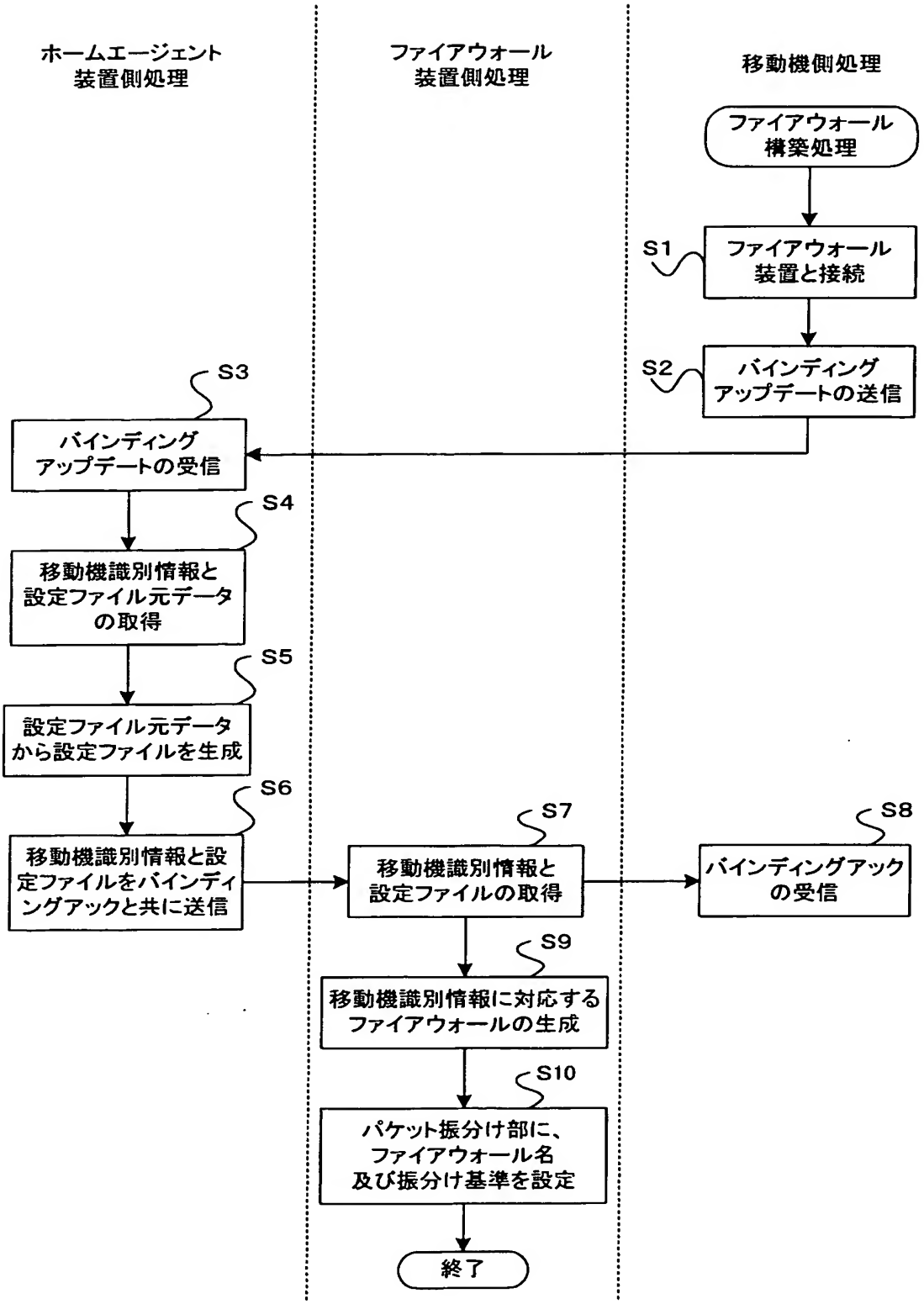
【図２】


ホームエージェント装置
10
11
設定ファイル元データ格納部
移動機識別情報
設定ファイル元データ
移動機50
ファイアウォール名等
移動機60
ファイアウォール名等
移動機70
ファイアウォール名等
BU受信部
12
設定ファイル送信部
13
バインディングアップデート
移動機識別情報＋設定ファイル

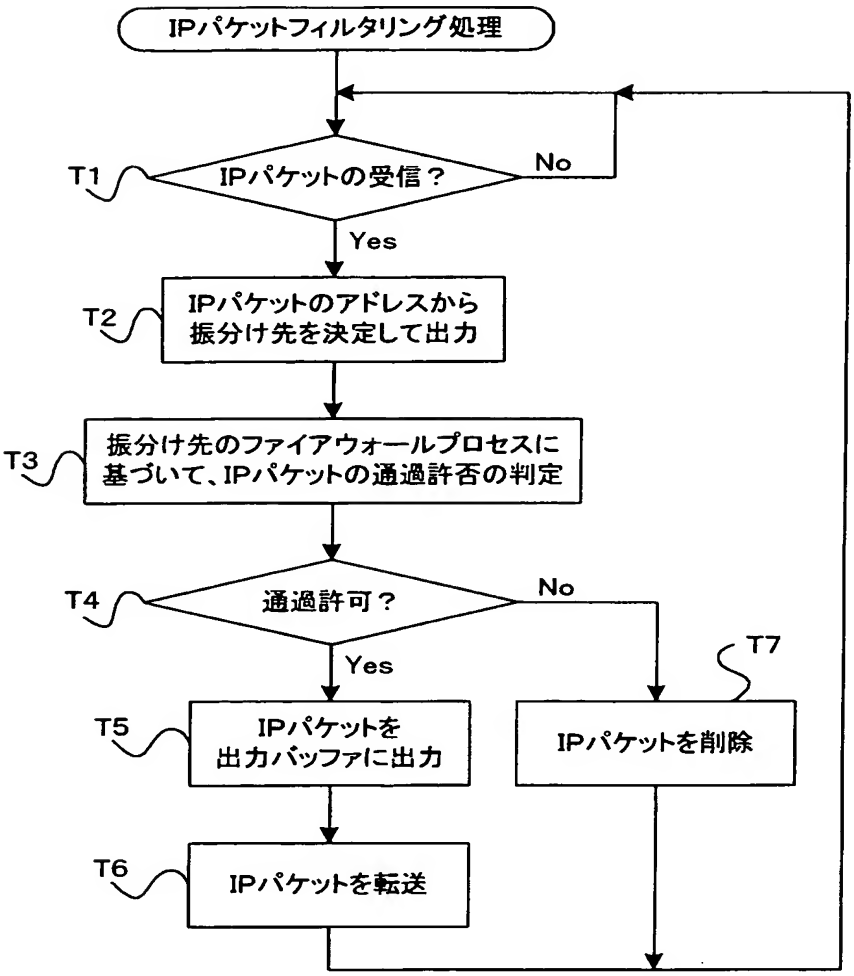
【図３】


50
移動機
IPパケット
IPパケット
23
出力バッファ
24
パケット振分け部
移動機50用のファイアウォールプロセス
移動機60用のファイアウォールプロセス
移動機70用のファイアウォールプロセス
223
221
222
ファイアウォール装置
21
パケット振分け部
25
出力バッファ
20
移動機識別情報＋設定ファイル
IPパケット
IPパケット
10
ホームエージェント装置

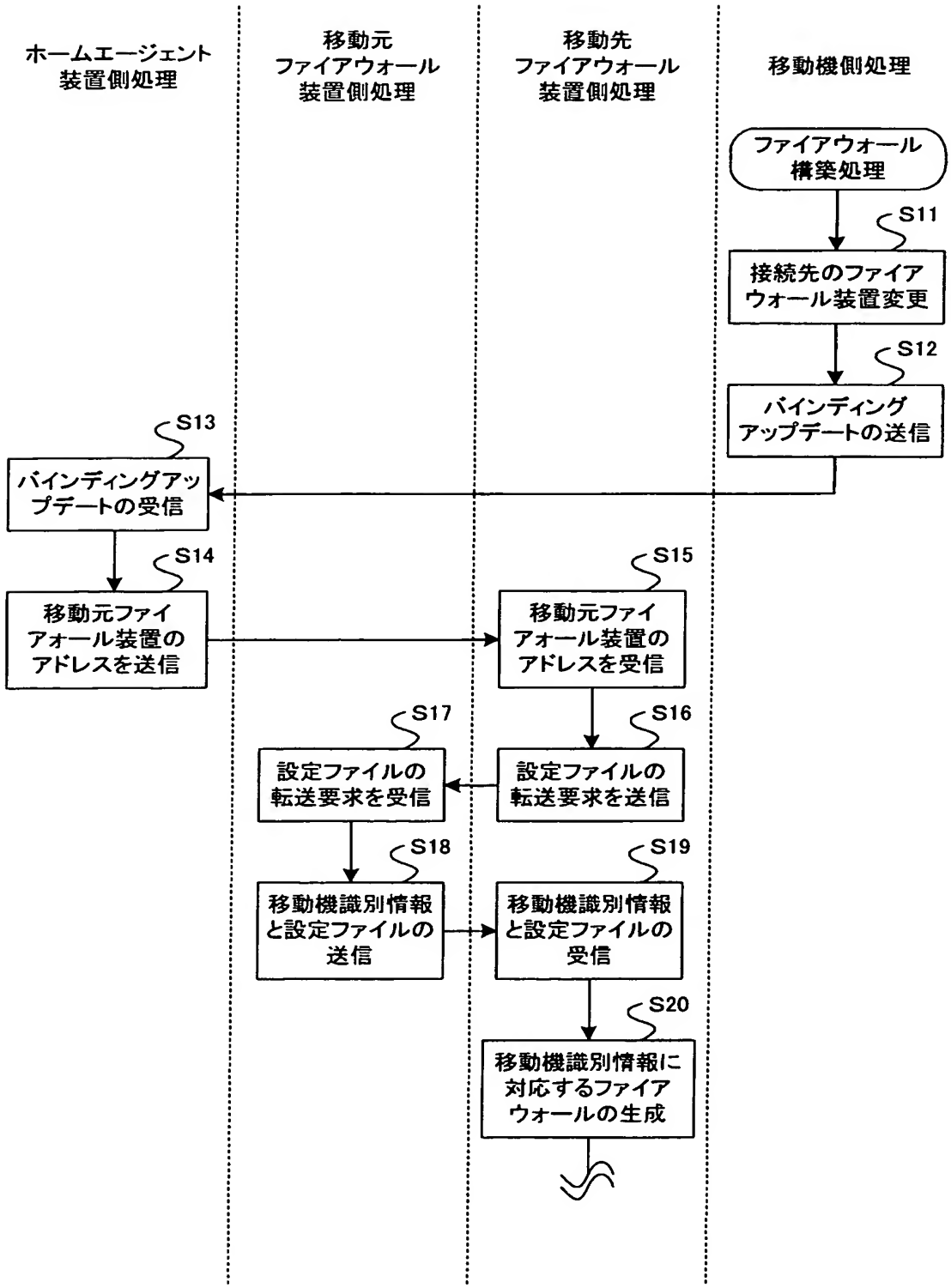
【図４】


ホームエージェント
装置側処理
ファイアウォール
装置側処理
移動機側処理
ファイアウォール
構築処理
S1
ファイアウォール
装置と接続
S2
バインディング
アップデートの送信
S3
バインディング
アップデートの受信
S4
移動機識別情報と
設定ファイル元データ
の取得
S5
設定ファイル元データ
から設定ファイルを生成
S6
移動機識別情報と設
定ファイルをバインディ
ングアックと共に送信
S7
移動機識別情報と
設定ファイルの取得
S8
バインディングアック
の受信
S9
移動機識別情報に対応する
ファイアウォールの生成
S10
パケット振分け部に、
ファイアウォール名
及び振分け基準を設定
終了

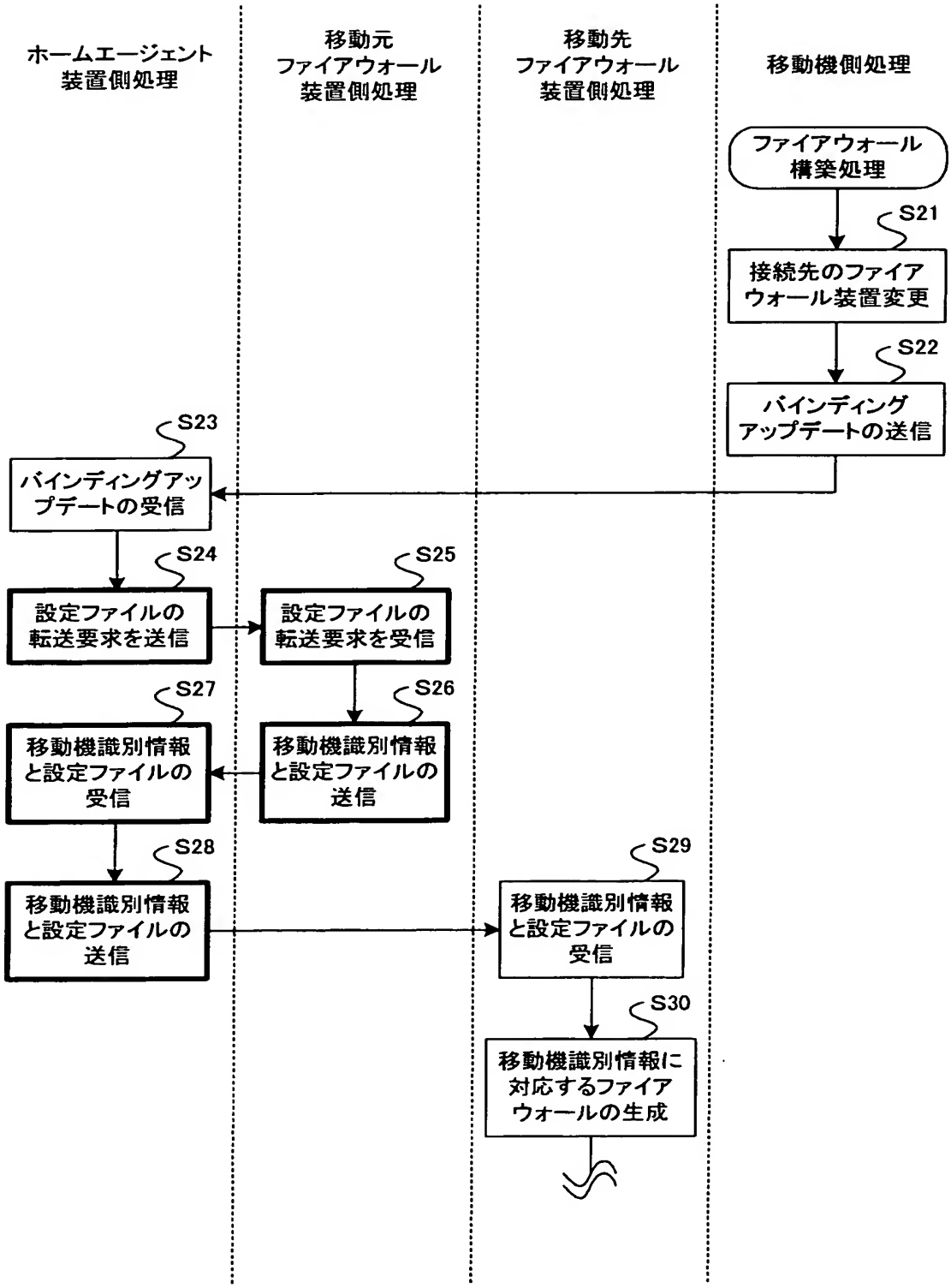
【図５】


IPパケットフィルタリング処理
T1
IPパケットの受信？
No
Yes
T2
IPパケットのアドレスから
振分け先を決定して出力
T3
振分け先のファイアウォールプロセスに
基づいて、IPパケットの通過許否の判定
T4
通過許可？
No
Yes
T7
T5
IPパケットを
出力バッファに出力
IPパケットを削除
T6
IPパケットを転送

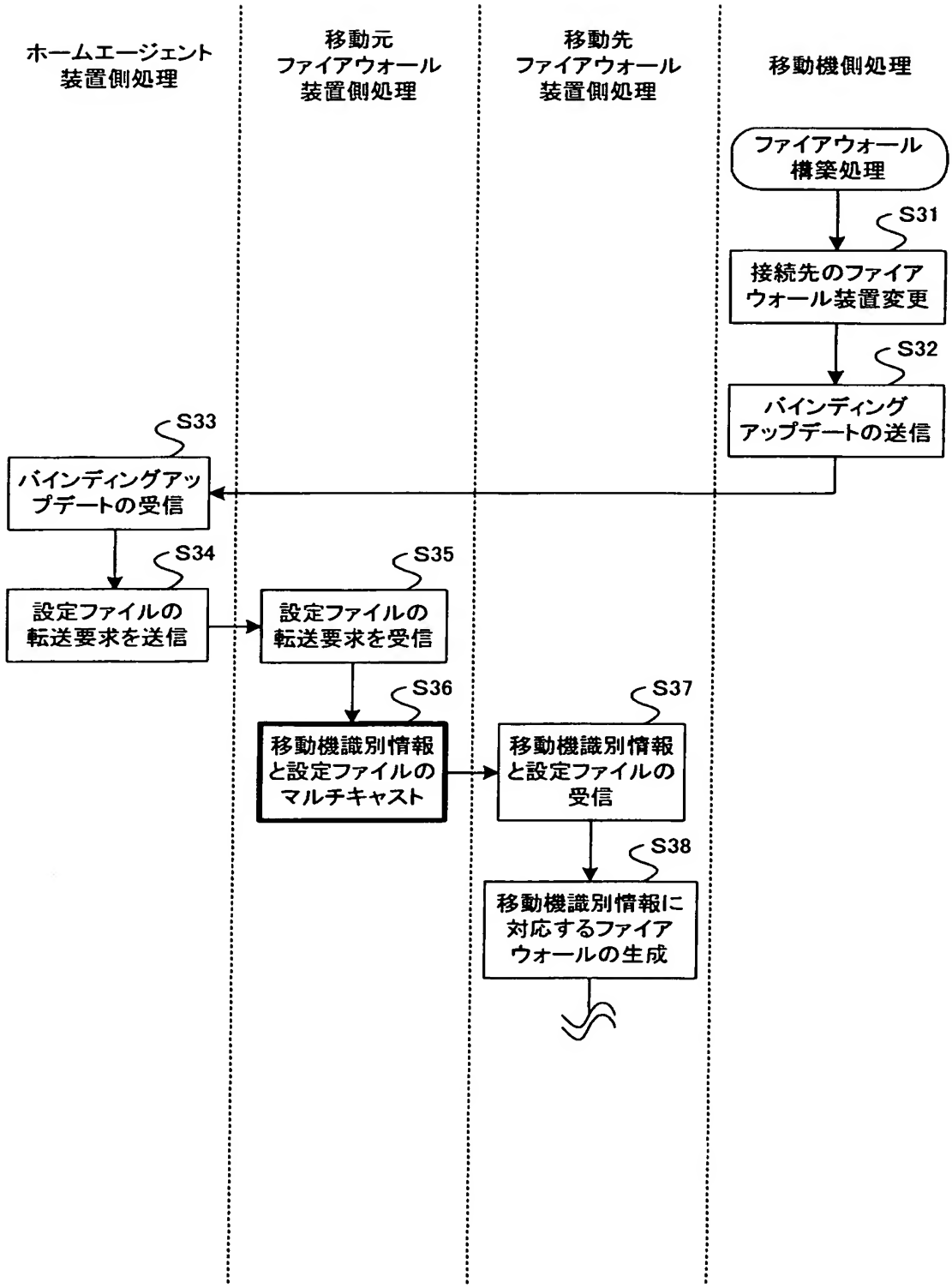
【図６】


ホームエージェント
装置側処理
移動元
ファイアウォール
装置側処理
移動先
ファイアウォール
装置側処理
移動機側処理
ファイアウォール
構築処理
S11
接続先のファイア
ウォール装置変更
S12
バインディング
アップデートの送信
S13
バインディングアッ
プデートの受信
S14
移動元ファイ
アォール装置の
アドレスを送信
S15
移動元ファイ
アォール装置の
アドレスを受信
S16
設定ファイルの
転送要求を送信
S17
設定ファイルの
転送要求を受信
S18
移動機識別情報
と設定ファイルの
送信
S19
移動機識別情報
と設定ファイルの
受信
S20
移動機識別情報に
対応するファイア
ウォールの生成

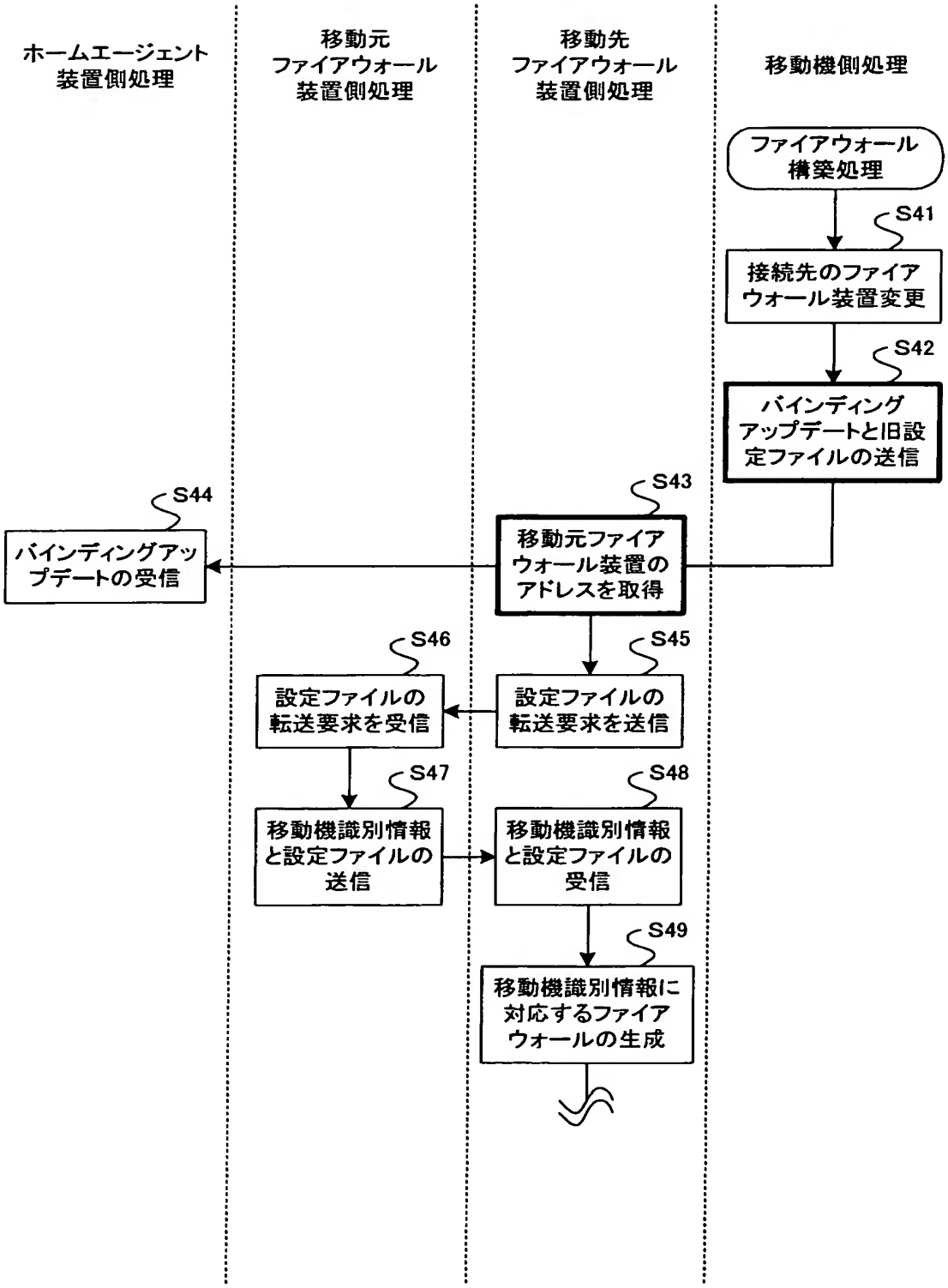
【図７】


ホームエージェント
装置側処理
移動元
ファイアウォール
装置側処理
移動先
ファイアウォール
装置側処理
移動機側処理
ファイアウォール
構築処理
S21
接続先のファイア
ウォール装置変更
S22
バインディング
アップデートの送信
S23
バインディングアッ
プデートの受信
S24
設定ファイルの
転送要求を送信
S25
設定ファイルの
転送要求を受信
S27
移動機識別情報
と設定ファイルの
受信
S26
移動機識別情報
と設定ファイルの
送信
S28
移動機識別情報
と設定ファイルの
送信
S29
移動機識別情報
と設定ファイルの
受信
S30
移動機識別情報に
対応するファイア
ウォールの生成

【図８】


ホームエージェント
装置側処理
移動元
ファイアウォール
装置側処理
移動先
ファイアウォール
装置側処理
移動機側処理
ファイアウォール
構築処理
S31
接続先のファイア
ウォール装置変更
S32
バインディング
アップデートの送信
S33
バインディングアッ
プデートの受信
S34
設定ファイルの
転送要求を送信
S35
設定ファイルの
転送要求を受信
S36
移動機識別情報
と設定ファイルの
マルチキャスト
S37
移動機識別情報
と設定ファイルの
受信
S38
移動機識別情報に
対応するファイア
ウォールの生成

【図９】


ホームエージェント装置側処理
移動元ファイアウォール装置側処理
移動先ファイアウォール装置側処理
移動機側処理
ファイアウォール構築処理
S41
接続先のファイアウォール装置変更
S42
バインディングアップデートと旧設定ファイルの送信
S43
移動元ファイアウォール装置のアドレスを取得
S44
バインディングアップデートの受信
S45
設定ファイルの転送要求を送信
S46
設定ファイルの転送要求を受信
S47
移動機識別情報と設定ファイルの送信
S48
移動機識別情報と設定ファイルの受信
S49
移動機識別情報に対応するファイアウォールの生成

【書類名】　要約書

【要約】

【課題】　移動機に対するファイアウォール機能の適用を可能とする

【解決手段】　本発明に係る通信制御システム１は、ホームエージェント装置１０と複数のファイアウォール装置２０～４０と移動機５０とを備える。移動機５０が例えばファイアウォール装置２０に接続すると、ファイアウォール装置２０は、移動機５０の識別情報及び設定ファイルをホームエージェント装置１０から受信し、設定ファイルを使用して、移動機５０用のファイアウォールを構築する。ファイアウォール装置２０は、ＩＰパケットを受信すると、当該パケットの宛先である移動機５０に適したファイアウォールを選定し、このファイアウォールに設定されているフィルタリング条件に従って通過許否の判定を行う。

【選択図】　図１

特願２００２－３４６２７１

出　願　人　履　歴　情　報

識別番号　　［３９２０２６６９３］

１．変更年月日　　２０００年　５月１９日
［変更理由］　　名称変更
住所変更
住　所　　東京都千代田区永田町二丁目１１番１号
氏　名　　株式会社エヌ・ティ・ティ・ドコモ